DRAFT − CUPS Software Security Report

CUPS−SSR−1.0

Easy Software Products

Table of Contents

1 Scope

1.1 Identification

This software security report provides an analysis of possible security concerns for the Common UNIX Printing System ("CUPS") Version 1.0.

1.2 System Overview

The Common UNIX Printing System provides a portable printing layer for UNIX® operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command−line interfaces.

CUPS uses the Internet Printing Protocol (IETF−IPP) as the basis for managing print jobs and queues. The Line Printer Daemon (LPD, RFC1179), Server Message Block (SMB), and AppSocket protocols are also supported with reduced functionality.

CUPS adds network printer browsing and PostScript Printer Description ("PPD")−based printing options to support real world applications under UNIX.

CUPS also includes a customized version of GNU GhostScript (currently based off GNU GhostScript 4.03) and an image file RIP that can be used to support non−PostScript printers.

1.3 Document Overview

This software security report is organized into the following sections:

- 1 − Scope
- 2 − References
- 3 − Local Access Risks
- 4 − Remote Access Risks
- A − Glossary

2 References

2.1 CUPS Documentation

The following CUPS documentation is referenced by this document:

- CUPS−CMP−1.0: CUPS Configuration Management Plan
- CUPS−IDD−1.0: CUPS System Interface Design Description
- CUPS−SAM−1.0.x: CUPS Software Administrators Manual
- CUPS−SDD−1.0: CUPS Software Design Description
- CUPS−SPM−1.0: CUPS Software Programming Manual
- CUPS−SSR−1.0: CUPS Software Security Report
- CUPS−STP−1.0: CUPS Software Test Plan
- CUPS−SUM−1.0.x: CUPS Software Users Manual
- CUPS−SVD−1.0.x: CUPS Software Version Description

2.2 Other Documents

The following non−CUPS documents are referenced by this document:

- IEEE 1387.4, System Administration: Printing (draft)
- IPP/1.0: Additional Optional Operations − Set 1
- RFC 1179, Line Printer Daemon Protocol
- RFC 2565, IPP/1.0: Encoding and Transport
- RFC 2566, IPP/1.0: Model and Semantics
- RFC 2639, IPP/1.0: Implementers Guide

3 Local Access Risks

Local access risks are those that can be exploited only with a local user account. This section does not address issues related to dissemination of the root password or other security issues associated with the UNIX operating system.

3.1 Security Breaches

There are two known security vulnerabilities with local access:

1. Since the default installation creates a world−readable request directory, it is possible for local users to read the contents of print files before they are printed.

   This problem can be alleviated by making the request directory readable only by the user specified in the CUPS configuration file.
2. Device URIs are passed to backend filters in argv[0] and in an environment variable. Since device URIs can contain usernames and passwords it may be possible for a local user to gain access to a remote resource.

   We recommend that any password−protected accounts used for remote printing have limited access priviledges so that the possible damages can be minimized.

   The device URI is "sanitized" (the username and password are removed) when sent to an IPP client so that a remote user cannot exploit this vulnerability.

4 Remote Access Risks

Remote access risks are those that can be exploited without a local user account and/or from a remote system. This section does not address issues related to network or firewall security.

4.1 Denial of Service Attacks

Like all Internet services, the CUPS server is vulnerable to denial of service attacks, including:

1. Establishing multiple connections to the server until the server will accept no more.

   This cannot be protected against by the current software. It is possible that future versions of the CUPS software could be configured to limit the number of connections allowed from a single host, however that still would not prevent a determined attack.
2. Repeatedly opening and closing connections to the server as fast as possible.

   There is no easy way of protecting against this in the CUPS software. If the attack is coming from outside the local network it might be possible to filter such an attack, however once the connection request has been received by the server it must at least accept the connection to find out who is connecting.
3. Flooding the network with broadcast packets on port 631.

   It might be possible to disable browsing if this condition is detected by the CUPS software, however if there are large numbers of printers available on the network such an algorithm might think that an attack was occurring when instead a valid update was being received.
4. Sending partial IPP requests; specifically, sending part of an attribute value and then stopping transmission.

   The current code is structured to read and write the IPP request data on−the−fly, so there is no easy way to protect against this for large attribute values.
5. Sending large/long print jobs to printers, preventing other users from printing.

   There are limited facilities for protecting against large print jobs (the `MaxRequestSize` attribute), however this will not protect printers from malicious users and print files that generate hundreds or thousands of pages. In general, we recommend restricting printer access to known hosts or networks, and adding user−level access control as needed for expensive printers.

4.2 Security Breaches

The current CUPS server only supports Basic authentication with usernames and passwords. This essentially places the clear text of the username and password on the network. Since CUPS uses the UNIX username and password account information, the authentication information could be used to gain access to accounts (possibly priviledged accounts) on the server.

The default CUPS configuration disables remote administration. We do not recommend that remote administration be enabled for all hosts, however if you have a trusted network or subnet access can be restricted accordingly.

The next minor release of CUPS will support Digest authentication of the entire message body using separate

MD5−based username and password files. This will protect password information and prevent unauthorized access due to compromised account passwords.

A Glossary

A.1 Terms

C

A computer language.

parallel

Sending or receiving data more than 1 bit at a time.

pipe

A one−way communications channel between two programs.

serial

Sending or receiving data 1 bit at a time.

socket

A two−way network communications channel.

A.2 Acronyms

ASCII

American Standard Code for Information Interchange

CUPS

Common UNIX Printing System

ESC/P

EPSON Standard Code for Printers

FTP

File Transfer Protocol

HP−GL

Hewlett−Packard Graphics Language

HP−PCL

Hewlett−Packard Printer Control Language

HP−PJL

Hewlett−Packard Printer Job Language

IETF

Internet Engineering Task Force

IPP

Internet Printing Protocol

ISO

International Standards Organization

LPD

Line Printer Daemon

MIME

Multimedia Internet Mail Exchange

PCL

Page Control Language

PPD

PostScript Printer Description

SMB

Server Message Block

TFTP

Trivial File Transfer Protocol